ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Number Theory 105 (2004) 235–250

JOURNAL OF Number Theory

http://www.elsevier.com/locate/jnt

Computation of the Iwasawa invariants of certain real abelian fields

Hiroki Sumida-Takahashi*,[1]

Faculty of Integrated Arts and Sciences, Hiroshima University, Kagamiyama, Higashi-Hiroshima 739-8521, Japan

Received 19 August 2002; revised 23 July 2003

Communicated by D. Goss

Abstract

Let p be a prime number and k a finite extension of $\mathbf{Q}$. It is conjectured that the Iwasawa invariants $\lambda_p(k)$ and $\mu_p(k)$ vanish for all p and totally real number fields k. Some methods to verify the conjecture for each real abelian field k are known, in which cyclotomic units and a set of auxiliary prime numbers are used. We give an effective method, based on the previous one, to compute the exact value of the other Iwasawa invariant $\nu_p(k)$ by using Gauss sums and another set of auxiliary prime numbers. As numerical examples, we compute the Iwasawa invariants associated to $k=\mathbf{Q}(\sqrt{f},\zeta_p+\zeta_p^{-1})$ in the range $1<f<200$ and $5\leqslant p<10\,000$.

MSC: 11R23

Keywords: Iwasawa invariant; Ideal class group; Cyclotomic unit; Gauss sum; Vandiver's conjecture; Greenberg's conjecture

1. Introduction

Let p be a prime number and k a finite extension of $\mathbf{Q}$. Denote by k_∞ the cyclotomic $\mathbf{Z}_p$-extension of k and by k_n the subfield of k_∞ such that $[k_n:k]=p^n$. Let

*Fax: +81-824-24-0756.

E-mail address: hiroki@mis.hiroshima-u.ac.jp.

[1] Partially supported by the Grants-in-Aid for Basic Science Research (No. 000101) from the Sumitomo Foundation. Partially supported by the Grants-in-Aid for Encouragement of Young Scientists (No. 13740015) from Japan Society for the Promotion of Science.

0022-314X/$ - see front matter © 2003 Elsevier Inc. All rights reserved.
doi:10.1016/j.jnt.2003.11.002

$A_n(k)$ be the p-Sylow subgroup of the ideal class group of k_n and $p^{e_n(k)}$ the order of $A_n(k)$. Iwasawa proved that there are three invariants $\lambda_p(k)$, $\mu_p(k)$ and $\nu_p(k)$ such that $e_n(k) = \lambda_p(k)n + \mu_p(k)p^n + \nu_p(k)$ for all sufficiently large n (cf. [17]).

It is conjectured that the μ-invariant vanishes for all p and k. In fact, Ferrero and Washington proved that $\mu_p(k) = 0$ for all p and abelian number fields k in [4]. As for the λ-invariant, there are many (non-totally real) number fields k with $\lambda_p(k) > 0$ (cf. [9, p. 266]). On the other hand, it is conjectured that $\lambda_p(k) = \mu_p(k) = 0$ for all p and totally real number fields k, which is called as Greenberg's conjecture. At present, we have numerical examples supporting this conjecture for abelian fields (e.g. [12,14,19,22]). In their methods, cyclotomic units and auxiliary prime numbers are used.

In [13], by a similar method, we verify $\lambda_p(k) = \mu_p(k) = 0$ for $p = 3, 5, 7$ and quadratic fields k with small discriminants, and give an upper bound for $\nu_p(k)$. However it is difficult to determine the exact value by the methods because we need to find a pth root of a cyclotomic unit (cf. [26, pp. 420–423]). The reason why we cannot determine the exact value in [13] is that we cannot tell which set of auxiliary prime numbers is effective to prove the existence of a pth root. In this paper, by using Gauss sums and another set of auxiliary prime numbers, we can find an effective set of auxiliary prime numbers and determine the exact value of the ν-invariant.

Using our method, we can settle the values of the tables in [13] by computer calculation. Moreover, we compute the Iwasawa invariants associated to $k = \mathbf{Q}(\sqrt{f}, \zeta_p + \zeta_p^{-1})$ in the range $1 < f < 200$ and $5 \leqslant p < 10\,000$, where f is the discriminant of a real quadratic field. We obtain some examples such that $\lambda_p(k) = \mu_p(k) = 0$ and $\nu_p(k) > 0$ for large prime numbers p. Let $\nu'_p(k) = \nu_p(k) - \nu_p(\mathbf{Q}(\zeta_p + \zeta_p^{-1})) - \varepsilon_p(k)$, where $\varepsilon_p(k)$ is the contribution to $\nu_p(k)$ from Dirichlet characters which do not satisfy (D2) in the next section. By the naive argument in [26, pp. 158–159], we deduce that the number of pairs (k, p) which satisfy $\nu'_p(k) > 0$ in the range $x_0 \leqslant p \leqslant x_1$ is approximately $\frac{1}{2}(\log\log x_1 - \log\log x_0)$. Our data does not seem to be much different from it.

2. Result

2.1. General case

We fix an inclusion map $\bar{\mathbf{Q}} \hookrightarrow \bar{\mathbf{Q}}_p$, where $\bar{F}$ is the algebraic closure of a field F. Further we fix a primitive nth root of unity ζ_n so that $\zeta_{nm}^m = \zeta_n$ for all $m, n \geqslant 1$. Let p be an odd prime number and f_0 an integer such that $p | f_0$ and $p^2 \nmid f_0$. Let K be a subfield of $\mathbf{Q}(\zeta_{f_0})$ containing ζ_p whose conductor is f_0. For simplicity, we assume the following condition:

(C1) p does not divide $|\mathrm{Gal}(K/\mathbf{Q})|$.

Put $f_n = f_0 p^n$. Then $K_n = K\mathbf{Q}_n \subseteq \mathbf{Q}(\zeta_{f_n})$. Further put $\Delta = \mathrm{Gal}(K_\infty/\mathbf{Q}_\infty)$, $\Gamma = \mathrm{Gal}(K_\infty/K)$ and $G_\infty = \mathrm{Gal}(K_\infty/\mathbf{Q}) = \Delta \times \Gamma$.

Let Φ be a $\mathbf{Q}_p$-valued character of Δ which is irreducible over $\mathbf{Q}_p$. Put

$$e_\Phi = \frac{1}{|\Delta|}\sum_{\delta\in\Delta} \Phi(\delta)\delta^{-1}$$

the idempotent of the group ring $\mathbf{Q}_p[\Delta]$. This is an element of $\mathbf{Z}_p[\Delta]$ by (C1). Let ϕ be an irreducible component of Φ over $\bar{\mathbf{Q}}_p$. We say Φ is even (resp. odd) when $\phi(\rho) = 1$ (resp. $\phi(\rho) = -1$), where ρ is the complex conjugate in Δ. Let $\mathcal{O}_\phi$ be the subring of $\bar{\mathbf{Q}}_p$ generated by all $\phi(\delta)$ ($\delta\in\Delta$) over $\mathbf{Z}_p$. We identify $e_\Phi \mathbf{Z}_p[\Delta]$ with $\mathcal{O}_\phi$ by $\delta \mapsto \phi(\delta)$.

We fix a topological generator γ_0 of Γ such that $\zeta_{f_n}^{\gamma_0} = \zeta_{f_n}^{1+f_0}$ for all $n \geqslant 0$. We identify, as usual, the complete group ring $\mathcal{O}_\phi[[\Gamma]]$ with the power series ring $\Lambda = \mathcal{O}_\phi[[T]]$ by $\gamma_0 = 1 + T$. Thus, for a $\mathbf{Z}_p[[G_\infty]]$-module M, we regard $M(\Phi) = e_\Phi M$ as a Λ-module. Let $X_\infty = X_\infty(K) = \lim_{\leftarrow} A_n(K)$, where the inverse limit is taken with respect to relative norm maps. Then $X_\infty(\Phi)$ is regarded as a Λ-module in the above way. We can define $e_n(\Phi)$, $\lambda_p(\Phi)$, $\mu_p(\Phi)$ and $\nu_p(\Phi)$ for $A_n(\Phi)$ and $X_\infty(\Phi)$. Let k be a subfield of K and $\phi(\delta) = 1$ for any $\delta \in \mathrm{Gal}(K/k)$. Then, since p does not divide $[K : k]$, $N_{K_n/k_n} : A_n(K)(\Phi) \to A_n(k)(\Phi)$ is an isomorphism.

From now on, let Ψ be a non-trivial *even* $\mathbf{Q}_p$-valued character of Δ which is irreducible over $\mathbf{Q}_p$ and ψ its fixed irreducible component of Ψ over $\bar{\mathbf{Q}}_p$. Put $\Psi^* = \Psi^{-1}\omega$ and $\psi^* = \psi^{-1}\omega$, where ω is the Teichmüller character $\mathbf{Z}/p\mathbf{Z} \to \mathbf{Z}_p$ ($\omega(a) \equiv a \bmod p$). We denote by $\mathcal{O}$ both $\mathcal{O}_\psi$ and $\mathcal{O}_{\psi^*}$. We fix a prime element π of $\mathcal{O}$.

Let $L_p(s, \psi)$ be the p-adic L-function associated to ψ which is constructed in [20]. By Iwasawa [16, Section 6], there uniquely exists $G_\Psi(T) \in \mathcal{O}[[T]]$ satisfying $G_\Psi((1 + f_0)^{1-s} - 1) = L_p(s, \psi)$ for all $s \in \mathbf{Z}_p$. In [4], it is shown that π does not divide $G_\Psi(T)$. Therefore, by the p-adic Weierstrass preparation theorem, we can uniquely write $G_\Psi(T) = g_\Psi(T)u_\Psi(T)$, where $g_\Psi(T)$ is a distinguished polynomial of $\mathcal{O}[T]$ and $u_\Psi(T)$ is an invertible element of $\mathcal{O}[[T]]$. In a similar way, we can define $g^*_\Psi(T) \in \mathcal{O}[T]$ from the power series $G^*_\Psi(T) \in \mathcal{O}[[T]]$ satisfying $G^*_\Psi((1 + f_0)^s - 1) = L_p(s, \psi)$. Put $\tilde{\lambda}(\Psi) = \deg g_\Psi(T) = \deg g^*_\Psi(T)$.

Further, for simplicity, we assume

$$\text{(C2)}\quad \psi(p) \neq 1 \text{ and } \psi^*(p) \neq 1.$$

For a non-negative integer n, we denote by p^{a_n} (resp. $p^{a^*_n}$) the exponent of $\Lambda/(\omega_n, g_\Psi(T))$ (resp. $\Lambda/(\omega_n, g^*_\Psi(T))$), where $\omega_n = (1 + T)^{p^n} - 1$. Since Leopoldt's conjecture holds for K_n and p [1,2], we have $a_n < \infty$. Further we have $a^*_n < \infty$ by (C2). Let $\mathbf{e}_{\Psi,n}$ (resp. $\mathbf{e}_{\Psi^*,n}$) be an element of $\mathbf{Z}[\Delta]$ such that $\mathbf{e}_{\Psi,n} \equiv e_\Psi \bmod p^{a_n}$ (resp. $\mathbf{e}_{\Psi^*,n} \equiv e_{\Psi^*} \bmod p^{a^*_n}$) and the sum of all the coefficients is zero. Put $N = N(n) = \max\{n, a_n - 1\}$ and $N^* = N^*(N) = \max\{N, a^*_N - 1\}$.

In [12], we define the following polynomials $X_n(T)\in\mathcal{O}[T]$ and $Y_n(T)\in\mathcal{O}[T]$:

$$X_n(T)g_\Psi(T)=p^{a_n}\quad\text{and}\quad Y_n(T)\equiv X_n(T)\bmod p^{a_n}.$$

In a similar way, we define $X_N^*(T)\in\mathcal{O}[T]$ and $Y_N^*(T)\in\mathcal{O}[T]$:

$$X_N^*(T)g_\Psi^*(T)=p^{a_N^*}\ \text{and}\ Y_N^*(T)\equiv X_N^*(T)\bmod p^{a_N^*}.$$

We define a cyclotomic unit c_n of K_n by

$$c_n=(N_{\mathbf{Q}(\zeta_{fn})/K_n}(1-\zeta_{f_n}))^{\mathbf{e}_{\Psi,n}}.$$

Let $\tilde{\mathcal{O}}_N$ be the ring of integers of $\mathbf{Q}(\zeta_{f_N})$ and $\tilde{\mathfrak{L}}$ a prime ideal of $\mathbf{Q}(\zeta_{f_N})$ with $\tilde{\mathfrak{L}}\nmid f_N$ which is lying above a prime number l. Denote by $\chi_{\tilde{\mathfrak{L}}}$ the character of $(\tilde{\mathcal{O}}_N/\tilde{\mathfrak{L}})^\times$ with values in $\langle\zeta_{f_N}\rangle$, defined by the following congruence:

$$\chi_{\tilde{\mathfrak{L}}}(y)=\chi_{\tilde{\mathfrak{L}}}(y\bmod\tilde{\mathfrak{L}})\equiv y^{(|\tilde{\mathcal{O}}_N/\tilde{\mathfrak{L}}|-1)/f_N}\bmod\tilde{\mathfrak{L}},\quad y\in\tilde{\mathcal{O}}_N\ \text{with}\ \tilde{\mathfrak{L}}\nmid y.$$

We define a Gauss sum $g'_N(\tilde{\mathfrak{L}})\in\mathbf{Q}(\zeta_{f_Nl})$ by

$$g'_N(\tilde{\mathfrak{L}})=-\sum_{y\in(\tilde{\mathcal{O}}_N/\tilde{\mathfrak{L}})^\times}\chi_{\tilde{\mathfrak{L}}}(y)\zeta_l^{\mathrm{Tr}(y)},$$

where Tr denotes the trace map: $\tilde{\mathcal{O}}_N/\tilde{\mathfrak{L}}\to\mathbf{Z}/l\mathbf{Z}$. Let $\mathfrak{A}$ be an ideal of K_N with $\mathfrak{A}\tilde{\mathcal{O}}_N=\prod_{i=1}^r\tilde{\mathfrak{L}}_i^{e_i}$, where $\tilde{\mathfrak{L}}_i$ is a prime ideal of $\mathbf{Q}(\zeta_{f_N})$ lying above l_i. We define a Gauss sum

$$g_N(\mathfrak{A})=\left(\prod_{i=1}^r g'_N(\tilde{\mathfrak{L}}_i)^{e_i}\right)^{f'\mathbf{e}_{\Psi^*,N}}\in K_N^\times,$$

where $f'=f_0/p$ (cf. [11,24, pp. 44–45; Proposition 3.1]).

Let $\mathfrak{L}$ (resp. $\mathfrak{L}^*$) be a prime ideal of K_N (resp. K_{N^*}) of degree 1 lying above a prime number l (resp. l^*). Put $F_{N,\mathfrak{L}}=(\mathcal{O}_N/\mathfrak{L})^\times/((\mathcal{O}_N/\mathfrak{L})^\times)^{p^{a_n}}$, $F_{N^*,\mathfrak{L}^*}=(\mathcal{O}_{N^*}/\mathfrak{L}^*)^\times/((\mathcal{O}_{N^*}/\mathfrak{L}^*)^\times)^{p^{a_N^*}}$, $F_{N,l}=\prod_{\mathfrak{L}|l}F_{N,\mathfrak{L}}$ and $F_{N^*,l^*}=\prod_{\mathfrak{L}^*|l^*}F_{N^*,\mathfrak{L}^*}$, where $\mathcal{O}_N$ is the ring of integers of K_N. For $L=\{l_i|1\leqslant i\leqslant s_0\}$ and $L^*=\{l_j^*|1\leqslant j\leqslant s^*\}$, let $K_N(L)$ (resp. $K_{N^*}(L^*)$) be the group of all elements of $K_N^\times$ (resp. $K_{N^*}^\times$) which are prime to all $l_i\in L$ (resp. $l_j^*\in L^*$). We define the following maps:

$$D_{N,L}:K_N(L)\to\prod_{i=1}^{s_0}F_{N,l_i}\quad(x\mapsto((x\bmod\mathfrak{L})\bmod((\mathcal{O}_N/\mathfrak{L})^\times)^{p^{a_n}})_{\mathfrak{L},i})$$

and

$$D^*_{N^*,L^*}:K_{N^*}(L^*)\to\prod_{j=1}^{s^*}F_{N^*,l_j^*}(x\mapsto((x\bmod\mathfrak{L}^*)\bmod((\mathcal{O}_{N^*}/\mathfrak{L}^*)^\times)^{p^{a_N^*}})_{\mathfrak{L}^*,j}).$$

We fix a prime ideal $\mathfrak{L}_i|l_i$ for each i. Put the first set of auxiliary prime ideals of K_N (resp. K_0): $L'=\{\mathfrak{L}_i|1\leqslant i\leqslant s_0\}$ (resp. $L'_0=\{\mathfrak{L}_{i,0}|\mathfrak{L}_{i,0}=N_{K_N/K_0}\mathfrak{L}_i,\ \mathfrak{L}_i\in L'\}$). For the if-part of Theorem 1, we will need to have $s_0\geqslant \dim_{\mathcal{O}/\pi} A_0(\Psi^*)/\pi A_0(\Psi^*)$.

We define a subset of cyclotomic units in K_n:

$$C'_n=\langle c_n^{T^m Y_n(T)}|0\leqslant m\leqslant s'_n\rangle_{\mathbf{Z}[\Delta]}$$

and a subset of Gauss sums in K_N:

$$G'_{N,L'}=\langle g_N(\mathfrak{L}_i)^{T^m Y_N^*(T)}|0\leqslant m\leqslant s'_N,\ 1\leqslant i\leqslant s_0\rangle_{\mathbf{Z}[\Delta]},$$

where $s'_n=\min\{\tilde{\lambda}(\Psi),p^n\}-1$. Let $L^*_{N^*(0)}$ be the second set of auxiliary prime ideals of $K_{N^*(0)}$ of degree 1. Using two local images, i.e. $D_{N,L}(C'_n)$ and $D_{N^*(0),L^*_{N^*(0)}}(G'_{0,L'_0})$, we can determine the exact order of $A_n(\Psi)$ in the following way.

Theorem 1. *Assume* (C1) *and* (C2). *Then*

$$|A_n(\Psi)|=p^{e_n(\Psi)}\leqslant\frac{|\Lambda/(g_\Psi(T),\omega_n)|}{|D_{N,L}(C'_n)|}.$$

If $|D^*_{N^*(0),L^*_{N^*(0)}}(G'_{0,L'_0})|=|\Lambda/(g^*_\Psi(T),\omega_0)|$ *for some* L'_0 *and* $L^*_{N^*(0)}$, *then the equality holds. Further, an equality* $e_m(\Psi)=e_{m+1}(\Psi)$ *implies that* $\lambda_p(\Psi)=\mu_p(\Psi)=0$ *and* $\nu_p(\Psi)=e_m(\Psi)$ *for any non-negative integer* m.

Proof. Let $K_{n,\mathfrak{P}_n}$ be the completion of K_n at $\mathfrak{P}_n|p$ and $\mathcal{U}_{\mathfrak{P}_n}$ the group of principal units of $K_{n,\mathfrak{P}_n}$. Put $\mathcal{U}_n=\prod_{\mathfrak{P}_n|p}\mathcal{U}_{\mathfrak{P}_n}$. Let d_n be the diagonal map:

$$d_n: K_n^\times\to\prod_{\mathfrak{P}_n|p}K_{n,\mathfrak{P}_n}^\times\quad(x\mapsto(x,x,\ldots,x)).$$

We denote by E_n the group of units of K_n and by C_n the group of cyclotomic units of K_n in the sense of [8]. Put

$$\mathcal{E}_n=\overline{\mathcal{U}_n\cap d_n(E_n)}\ \text{and}\ \mathcal{C}_n=\overline{\mathcal{U}_n\cap d_n(C_n)},$$

where $\bar{A}$ is the topological closure in $\mathcal{U}_n$. By (C2) and [8, Theorem 2], we have the following Λ-isomorphisms:

$$\begin{array}{ccc}\mathcal{U}_n(\Psi) & \simeq & \Lambda/(\omega_n)\\ \bigcup| & & \bigcup|\\ \mathcal{E}_n(\Psi) & \simeq & V_n\\ \bigcup| & & \bigcup|\\ \mathcal{C}_n(\Psi) & \simeq & (g_\Psi(T),\omega_n)/(\omega_n).\end{array}$$

By the Iwasawa main conjecture proved in [10,23,27], we have

$$\begin{aligned} p^{e_n(\Psi)} &= |A_n(\Psi)| = |\mathscr{E}_n(\Psi)/\mathscr{C}_n(\Psi)| = |\mathscr{U}_n(\Psi)/\mathscr{C}_n(\Psi)|/|\mathscr{U}_n(\Psi)/\mathscr{E}_n(\Psi)| \\ &= |\Lambda/(g_\Psi(T),\omega_n)|/|\mathscr{U}_n(\Psi)^{p^{a_n}}/\mathscr{E}_n(\Psi)^{p^{a_n}}| \\ &= |\Lambda/(g_\Psi(T),\omega_n)|/|\mathscr{C}'_n(\Psi)/\mathscr{E}_n(\Psi)^{p^{a_n}}|, \end{aligned}$$

where $\mathscr{C}'_n = \overline{\mathscr{U}_n \cap (d_n(C'_n)\mathscr{C}_n^{p^{a_n}})}$. Leopoldt's conjecture implies that $E_n/E_n^{p^{a_n}} \simeq \mathscr{E}_n/\mathscr{E}_n^{p^{a_n}}$. Hence we have the following map:

$$(C'_n E_n^{p^{a_n}}/E_n^{p^{a_n}})(\Psi) \simeq \mathscr{C}'_n(\Psi)/\mathscr{E}_n(\Psi)^{p^{a_n}} \to D_{N,L}(C'_n).$$

Since this map is surjective, the first assertion of the theorem follows. We will show that it is an isomorphism if $|D^*_{N^*(0),L^*_{N^*(0)}}(G'_{0,L'_0})| = |\Lambda/(g^*_\Psi(T),\omega_0)|$. Denote by τ the canonical isomorphism:

$$\tau : (\mathbf{Z}/f_N l\mathbf{Z})^\times \to \mathrm{Gal}(\mathbf{Q}(\zeta_{f_N l})/\mathbf{Q}) \quad (m \bmod f_N l \mapsto \tau_m \ (\zeta_{f_N l}^{\tau_m} = \zeta_{f_N l}^m)).$$

Put

$$\theta_N = \sum_{1 \leqslant m < f_N,\ (m,f_N)=1} \left(1 - \frac{m}{f_N}\right) \tau_{m|K_N} \in \mathbf{Q}[\mathrm{Gal}(K_N/\mathbf{Q})].$$

By Stickelberger's theorem [24, Proposition 3.1], for any sufficiently large m, there exists $g' \in K_N^\times$ such that

$$(g_N(\mathfrak{Q}_i)) = \mathfrak{Q}_i^{f' \mathbf{e}_{\Psi^*,m}\theta_N}(g'^{p^{a^*_N}}).$$

We have

$$\begin{aligned} &\mathbf{e}_{\Psi^*,m}\theta_N Y^*_N(T) \\ &\quad = (e_{\Psi^*} + p^m Z)\theta_N Y^*_N(T) \\ &\quad \equiv g^*_\Psi(T)u(T)(X^*_N(T) + p^{a^*_N} W(T))e_{\Psi^*} + p^m Z\theta_N Y^*_N(T) \bmod \omega_N \\ &\quad \equiv p^{a^*_N}(1 + W(T)g^*_\Psi(T))u(T)e_{\Psi^*} + p^m Z\theta_N Y^*_N(T) \bmod \omega_N \end{aligned}$$

for some $Z \in \mathbf{Z}_p[\Delta]$, $W(T) \in \mathcal{O}[T]$ and $u(T) \in \mathcal{O}[[T]]^\times$. Let L_N be the maximal unramified abelian p-extension of K_N. Let $L_N(\Psi^*)$ be the subfield of L_N corresponding to $\prod_{\Phi \neq \Psi^*} \mathrm{Gal}(L_N/K_N)(\Phi)$, where Φ runs over every $\mathbf{Q}_p$-valued character of Δ which is irreducible over $\mathbf{Q}_p$. We denote by $\left(\frac{L_N/K_N}{\mathfrak{Q}_i}\right)$ the Artin symbol.

Put

$$\sigma_{\mathfrak{L}_i} = \left(\frac{L_N(\Psi^*)/K_N}{\mathfrak{L}_i}\right) = \left(\frac{L_N(\Psi^*)/K_N}{\mathfrak{L}_i}\right)^{e_{\Psi^*}} = \left(\frac{L_N/K_N}{\mathfrak{L}_i}\right)^{e_{\Psi^*}}_{|L_N(\Psi^*)}.$$

Then, by Stickelberger's theorem, we have $\sigma_{\mathfrak{L}_i}^{g^*_{\Psi}(T)} = 1$. Let us consider the following maps:

$$\begin{aligned} A_N(\Psi^*) &\to K_N^\times/(K_N^\times)^{p^{a^*_N}} \quad (Cl(\mathfrak{U}) \mapsto \alpha^{\mathbf{e}_{\Psi^*,N}} \bmod (K_N^\times)^{p^{a^*_N}}) \\ &\to K_{N^*}^\times/(K_{N^*}^\times)^{p^{a^*_N}} \supseteq K_{N^*}(L^*)(K_{N^*}^\times)^{p^{a^*_N}}/(K_{N^*}^\times)^{p^{a^*_N}} \\ &\simeq K_{N^*}(L^*)/(K_{N^*}(L^*))^{p^{a^*_N}} \to \prod_{j=1}^{s^*} F_{N^*,l_j^*}, \end{aligned}$$

where $\alpha \in K_N^\times$ such that $\mathfrak{U}^{p^{a^*_N}} = (\alpha)$. Since Ψ is not trivial and $p \neq 2$, the first map is well-defined. By the proposition below,

$$|D^*_{N^*(0),L^*_{N^*(0)}}(G'_{0,L'_0})| = |\Lambda/(g^*_{\Psi}(T), \omega_0)|$$

implies that

$$|D^*_{N^*,L^*}(G'_{N,L'})| = |\Lambda/(g^*_{\Psi}(T), \omega_N)| = |A_N(\Psi^*)|$$

for some L^*. By the above maps, we have

$$\langle Cl(\mathfrak{L}_i)^{qe_{\Psi^*}T^m} | 0 \leqslant m \leqslant s'_N,\ 1 \leqslant i \leqslant s_0 \rangle_{\mathbf{Z}[\Delta]} = A_N(\Psi^*)$$

for some integer q such that $p \nmid q$. By the class field theory, this implies that

$$\langle \sigma_{\mathfrak{L}_i}^{T^m} | 0 \leqslant m \leqslant s'_N,\ 1 \leqslant i \leqslant s_0 \rangle_{\mathbf{Z}[\Delta]} = \mathrm{Gal}(L_N(\Psi^*)/K_N).$$

For $c \in C'_n$, since $d_n(c) \in \mathscr{C}'_n(\Psi)E_n^{p^{a_n}} \subseteq \mathscr{U}_n^{p^{a_n}}$, $K_N(\sqrt[p^{a_n}]{c}) \subseteq L_N(\Psi^*)$. Furthermore, because $\{\sigma_{\mathfrak{L}_i} |\ 1 \leqslant i \leqslant s_0\}$ generate $\mathrm{Gal}(L_N(\Psi^*)/K_N)$ over Λ, $K_N(\sqrt[p^{a_n}]{c}) = K_N$ (i.e. $c \in (K_N^\times)^{p^{a_n}}$) if and only if $c \bmod \mathfrak{L} \in ((\mathscr{O}_N/\mathfrak{L})^\times)^{p^{a_n}}$ for all $\mathfrak{L}|l_i$ and $l_i \in L$. This implies that $\mathscr{C}'_n(\Psi)/\mathscr{E}_n(\Psi)^{p^{a_n}} \simeq D_{N,L}(C'_n)$. Therefore the above assertion follows.

By (C2), we have $A_n(\Psi) \simeq X_\infty(\Psi)/\omega_n X_\infty(\Psi)$ (cf. [12, p. 731]). If $|A_m(\Psi)| = |A_{m+1}(\Psi)|$, then $\omega_m X_\infty(\Psi) = \omega_{m+1}X_\infty(\Psi) \subseteq (p, T)\omega_m X_\infty(\Psi)$. By Nakayama's lemma, we have $\omega_m X_\infty(\Psi) = 0$. Therefore $A_n(\Psi) \simeq X_\infty(\Psi)$ for $n \geqslant m$ and the last assertion follows. □

Proposition 1. *In the above setting,* $|D^*_{N^*,L^*}(G'_{N,L'})| = |\Lambda/(g^*_{\Psi}(T), \omega_N)|$ *holds for some* L^* *if and only if* $|D^*_{N^*(0),L^*_{N^*(0)}}(G'_{0,L'_0})| = |\Lambda/(g^*_{\Psi}(T), \omega_0)|$ *holds for some* $L^*_{N^*(0)}$.

Proof. By the main conjecture and (C2), we have $|A_N(\Psi^*)| = |\Lambda/(g^*_\Psi(T), \omega_N)|$. Therefore, as in the proof of Theorem 1, if

$$|D^*_{N^*,L^*}(G'_{N,L'})| = |\Lambda/(g^*_\Psi(T), \omega_N)|,$$

then

$$\langle \sigma_{\mathfrak{Q}_i}^{T^m} | 0 \leqslant m \leqslant s'_N,\ 1 \leqslant i \leqslant s_0 \rangle_{\mathbf{Z}[\Delta]} = \mathrm{Gal}(L_N(\Psi^*)/K_N).$$

By Nakayama's lemma and

$$\sigma_{\mathfrak{Q}_i}|_{L_0(\Psi^*)} = \left(\frac{L_0(\Psi^*)/K_0}{N_{K_N/K_0}\mathfrak{Q}_i}\right) = \left(\frac{L_0(\Psi^*)/K_0}{\mathfrak{Q}_{i,0}}\right) = \sigma_{\mathfrak{Q}_{i,0}},$$

we have

$$\langle \sigma_{\mathfrak{Q}_i}^{T^m} | 0 \leqslant m \leqslant s'_N,\ 1 \leqslant i \leqslant s_0 \rangle_{\mathbf{Z}[\Delta]} = \mathrm{Gal}(L_N(\Psi^*)/K_N)$$

if and only if

$$\langle \sigma_{\mathfrak{Q}_{i,0}} | 1 \leqslant i \leqslant s_0 \rangle_{\mathbf{Z}[\Delta]} = \mathrm{Gal}(L_0(\Psi^*)/K_0).$$

The Chebotarev density theorem guarantees existence of L^* and $L^*_{N^*(0)}$ when the above equalities hold. □

2.2. Special case

We explain how to use the criterion in practice. Following [13], we consider the following case.

(D1) The exponent of $\mathrm{Gal}(K/\mathbf{Q})$ divides $p-1$.

(D2) $\psi(p) \neq 1$ and $\psi^*(p) \neq 1$.

(D3) $g_\psi(T) = T - \alpha$ for some $\alpha \in p\mathbf{Z}_p$.

By (D1), the values of ψ are contained in $\mathbf{Z}_p$ and $\Psi = \psi$. Put $\alpha^* = \frac{f_0 - \alpha}{1+\alpha} \in p\mathbf{Z}_p$, $e = v_p(\alpha)$ and $e^* = v_p(\alpha^*)$, where v_p is the p-adic valuation such that $v_p(p) = 1$. Then we have $a_n = n + e$, $a^*_n = n + e^*$, $N = N(n) = n + e - 1$, $N^* = N^*(N) = N + e^* - 1 = n + e + e^* - 2$ and $0 \leqslant e_n(\psi) \leqslant n + e$. Further

$$X_n(T) = \frac{\omega_n(T) - \omega_n(\alpha)}{T - \alpha} u \text{ and } Y_n(T) \equiv X_n(T) \bmod p^{n+e}$$

and

$$X_N^*(T) = \frac{\omega_N(T) - \omega_N(\alpha^*)}{T - \alpha^*} u^* \text{ and } Y_N^*(T) \equiv X_N^*(T) \bmod p^{N+e^*},$$

where $u = \frac{p^{n+e}}{1-(1+\alpha)^{p^{n}}}$ and $u^* = \frac{p^{N+e^*}}{1-(1+\alpha^*)^{p^N}}$.

Let $\mathfrak{L}$ (resp. $\mathfrak{L}^*$) be a prime ideal of K_N (resp. K_{N^*}) of degree 1 lying above a prime number l (resp. l^*). Put

$$D_{N,\mathfrak{L}} : K_N(\mathfrak{L}) \to F_{N,\mathfrak{L}} \text{ and } D^*_{N^*,\mathfrak{L}^*} : K_{N^*}(\mathfrak{L}^*) \to F_{N^*,\mathfrak{L}^*}.$$

By (D3), we have $\sigma_{\mathfrak{L}}^{\gamma_0} = \sigma_{\mathfrak{L}}^{1+\alpha^*}$. Further we have $\sigma_{\mathfrak{L}}^{\delta} = \sigma_{\mathfrak{L}}^{\psi^*(\delta)}$ for $\delta \in \Delta$. Hence the orders of $D_{N,\mathfrak{L}}(C_n')$ and $D^*_{N^*,\mathfrak{L}^*}(G'_{N,\mathfrak{L}})$ depend only on l and l^*. So we can write

$$|D_{N,l}(C_n')| = |D_{N,\mathfrak{L}}(C_n')| \text{ and } |D^*_{N^*,l^*}(G'_{N,l})| = |D^*_{N^*,\mathfrak{L}^*}(G'_{N,\mathfrak{L}})|.$$

In this case, we can write Theorem 1 as follows.

Theorem 2. *Assume* (D1)–(D3). *For any prime number l which splits completely in $K_{n+e-1}/\mathbf{Q}$,*

$$|A_n(\psi)| \leqslant \frac{p^{n+e}}{|D_{n+e-1,l}(C_n')|}.$$

If $|D^*_{e^*-1,l^*_{e^*-1}}(G'_{0,l})| = p^{e^*}$ for some $l^*_{e^*-1}$ which splits completely in $K_{e^*-1}/\mathbf{Q}$, then the equality holds. If $e_m(\psi) = m + e - 1$ for some m, then $\lambda_p(\psi) = \mu_p(\psi) = 0$ and $\nu_p(\psi) = m + e - 1$.

3. Computation of the Gauss sum modulo a prime ideal

Let l (resp. l^*) be a prime number such that $l \equiv 1 \bmod f_N$ (resp. $l^* \equiv 1 \bmod f_N l$), and g (resp. g^*) a primitive root in $\mathbf{Z}/l\mathbf{Z}$ (resp. $\mathbf{Z}/l^*\mathbf{Z}$). Let s (resp. t) be an integer satisfying $s \equiv g^{*(l^*-1)/f_N} \bmod l^*$ (resp. $t \equiv g^{*(l^*-1)/l} \bmod l^*$). Then, for some ideal $\mathfrak{L}|l$ of K_N and $\mathfrak{L}^*|l^*$ of $K_N(\zeta_l)$, $s \equiv \chi_{\mathfrak{L}}(g) \bmod \mathfrak{L}^*$ and $t \equiv \zeta_l \bmod \mathfrak{L}^*$. We write

$$Y_N^*(T) = \sum_{j=0}^{p^N-1} a_j (1+T)^j = \sum_{j=0}^{p^N-1} a_j \gamma_0^j, \quad a_j \in \mathbf{Z}.$$

We here identify $\mathrm{Gal}(K_N/K_0)$ (resp. $\mathrm{Gal}(K_N/\mathbf{Q}_N)$) with $\mathrm{Gal}(K_N(\zeta_l)/K_0(\zeta_l))$ (resp. $\mathrm{Gal}(K_N(\zeta_l)/\mathbf{Q}_N(\zeta_l))$). Let $\mathfrak{A}_N$ be the subgroup of $(\mathbf{Z}/f_N l\mathbf{Z})^\times$ which is corresponding to $\mathrm{Gal}(\mathbf{Q}(\zeta_{f_N l})/\mathbf{Q}_N(\zeta_l))$ by the isomorphism τ. Taking an extension to

$\mathrm{Gal}(\mathbf{Q}(\zeta_{f_N l})/\mathbf{Q}_N(\zeta_l))$, we write

$$\left(\sum_{\tau\in \mathrm{Gal}(\mathbf{Q}(\zeta_{f_N})/K_N)} \tau\right)\mathbf{e}_{\Psi^*,N} = \sum_{m\in\mathfrak{U}_N} b_m\tau_m, \quad b_m\in\mathbf{Z}.$$

Then we have

$$\begin{aligned} g_N(\mathfrak{Q})^{Y_N^*(T)} &= \left(\prod_{j=0}^{p^N-1}\left(\prod_{m\in\mathfrak{U}_N}\left(-\sum_{y\in(\mathcal{O}_N/\mathfrak{Q})^\times}\chi_{\mathfrak{Q}}(y)\zeta_l^y\right)^{b_m\tau_m}\right)^{a_j\gamma_0^j}\right)^{f'} \\ &\equiv \left(\prod_{0\leqslant j<p^N,\ m\in\mathfrak{U}_N}\left(-\sum_{i=0}^{l-2} s^{m(1+f_0)^j i}t^{g^i}\right)^{b_m a_j}\right)^{f'} \bmod \mathfrak{Q}^*. \end{aligned}$$

In order to compute the above sums, it suffices to compute the following discrete Fourier transforms:

$$F(w) = \sum_{0\leqslant v<z}\zeta_z^{wv}f(v) = \zeta_{2z}^{w^2}\sum_{0\leqslant v<z}\zeta_{2z}^{-(v-w)^2}(\zeta_{2z}^{v^2}f(v))$$

for $0\leqslant w<z$, where $z=f_N$ and $f(v)=\sum_{0\leqslant i<l-1,\ i\equiv v \bmod f_N} t^{g^i}$. Assume $l^*\equiv 1 \bmod 2f_N l$. Since

$$\sum_{i=0}^{n-1}a_i x^i\sum_{j=0}^{n-1}b_j x^j = \sum_{k=0}^{n-1}\left(\sum_{i=0}^{n-1}a_{i \bmod n}b_{(k-i) \bmod n}\right)x^k \in (\mathbf{Z}/l^*\mathbf{Z})[x]/(x^n-1),$$

we can calculate the above convolutions from a multiplication of two polynomials, or natural numbers. By using the fast Fourier transformation repeatedly, Schönhage and Strassen showed that it is possible to multiply two n-bit numbers in $O(n\log n\log\log n)$ steps (cf. [18, 4.3.3]). By a similar method, we can effectively compute the Gauss sum modulo a prime ideal by a computer with a sufficiently large memory.

There are other computations to find a pth root of the cyclotomic unit in [6,19]. These computations become much more difficult as the prime number p or the extension degree of the field containing the cyclotomic unit is larger. It is necessary to do the computations with extremely accurate approximations of the cyclotomic unit.

4. Numerical examples

4.1. $\mathbf{Q}(\sqrt{f})$

Let p be an odd prime number and k the real quadratic field whose discriminant is f. Let φ_f be the non-trivial Dirichlet character associated to $k=\mathbf{Q}(\sqrt{f})$. Put $K=\mathbf{Q}(\sqrt{f},\zeta_p)$. Then we have $A_n(k)=A_n(k)(\varphi_f)\simeq A_n(K)(\varphi_f)$ by Iwasawa [15]. The following examples satisfy (D1)–(D3) for $p=3$.

$f=29$: By computation, we have

$$\begin{cases}\alpha\equiv 18 \bmod p^3, & e=2\\ \alpha^*\equiv 15 \bmod p^3, & e^*=1.\end{cases}$$

Since $|D_{1,l}(C_0')|=p^2$ for $l=523$, we have $|A_0(\varphi_f)|\leqslant p^{2-2}=1$ by Theorem 2. Therefore we obtain

$$e_0=e_1=e_2=\cdots\leq(=)0 \text{ and } \lambda_p(k)=\mu_p(k)=\nu_p(k)=0.$$

In this case, we do not need to calculate any Gauss sum.

$f=761$: By computation, we have

$$\begin{cases}\alpha\equiv 3 \bmod p^2, & e=1,\\ \alpha^*\equiv 3 \bmod p^2, & e^*=1.\end{cases}$$

Though $|D_{0,l}(C_0')|=1$ for some prime numbers l, $|D_{1,l}(C_1')|=p$ for $l=237\,397$. Hence we have $|A_n(\varphi_f)|\leqslant p^{2-1}=p$ for $n\geqslant 1$ by Theorem 2.

Since $|D^*_{0,l_0^*}(G_{0,l})|=p$ and $|D_{0,l}(C_0')|=1$ for $l=4567$ and $l_0^*=62\,558\,767$, we have $|A_0(\varphi_f)|=p$ by Theorem 2. Therefore we obtain

$$e_0=e_1=e_2=\cdots=1,\ \lambda_p(k)=\mu_p(k)=0 \text{ and } \nu_p(k)=1.$$

$f=473$: By computation, we have

$$\begin{cases}\alpha\equiv 30 \bmod p^5, & e=1,\\ \alpha^*\equiv 84 \bmod p^5, & e^*=1.\end{cases}$$

Though $|D_{n,l}(C_n')|=1$ for $n\leqslant 4$ and some prime numbers l, $|D_{5,l}(C_5')|=p$ for $l=2\,068\,903$. Hence we have $|A_n(\varphi_f)|\leqslant p^{6-1}=p^5$ for $n\geqslant 5$ by Theorem 2.

Since $|D^*_{0,l_0^*}(G_{0,l})|=p$ and $|D_{4,l}(C_4')|=1$ for $l=1\,609\,147$ and $l_0^*=22\,833\,795\,931$, we have $|A_4(\varphi_f)|=p^5$ by Theorem 2. Therefore we obtain

$$e_n=n+1 \quad \text{for } n\leqslant 4, \quad e_n=5 \quad \text{for } n\geqslant 5,\ \lambda_p(k)=\mu_p(k)=0 \text{ and } \nu_p(k)=5.$$

By the above procedure, we can settle the value in [13].

4.2. $\mathbf{Q}(\sqrt{f}, \zeta_p + \zeta_p^{-1})$

Vandiver's conjecture claims that $\lambda_p(k) = \mu_p(k) = \nu_p(k) = 0$ for all $k = \mathbf{Q}(\zeta_p + \zeta_p^{-1})$. By computer calculation, this conjecture is verified for $p < 12\,000\,000$ [3]. We here replace $\mathbf{Q}$ with $\mathbf{Q}(\sqrt{f})$ and consider the Iwasawa invariants associated to $k = \mathbf{Q}(\sqrt{f}, \zeta_p + \zeta_p^{-1})$ and $K = \mathbf{Q}(\sqrt{f}, \zeta_p)$, where f is the discriminant of a real quadratic field.

In the range $1 < f < 200$, $5 \leqslant p < 10\,000$ and $2 \leqslant 2i \leqslant p - 3$, there are 171 981 262 pairs of $(\varphi_f \omega^{2i}, p)$ which satisfy (D1) and (D2). Among them, there are 37 140 pairs with $\tilde{\lambda}_p(\varphi_f \omega^{2i}) = 1$, 46 pairs with $\tilde{\lambda}_p(\varphi_f \omega^{2i}) = 2$, and two pairs with $\tilde{\lambda}_p(\varphi_f \omega^{2i}) = 3$. We verified Greenberg's conjecture $\lambda_p(\varphi_f \omega^{2i}) = \mu_p(\varphi_f \omega^{2i}) = 0$ for each of them by the method in [12]. Except for $(\varphi_{177}\omega^6, 17)$, we verified it by using cyclotomic units of k_0 or k_1. For $(\varphi_{177}\omega^6, 17)$, we used cyclotomic units of k_2 to verify it. In the above range, there are 38 pairs which do not satisfy (D2). We also verified the conjecture for each of them. Furthermore, by Fukuda's extended computation of p-units of real quadratic fields $\mathbf{Q}(\sqrt{f})$, we can verify that $\lambda_p(\varphi_f) = \mu_p(\varphi_f) = 0$ for $1 < f < 200$ and $5 \leqslant p < 10\,000$ (cf. [5,7]).

Proposition 2. *$\lambda_p(\mathbf{Q}(\sqrt{f}, \zeta_p + \zeta_p^{-1})) = \mu_p(\mathbf{Q}(\sqrt{f}, \zeta_p + \zeta_p^{-1})) = 0$ for all $1 < f < 200$ and $5 \leqslant p < 10\,000$.*

In the following tables, we give lists of $(f, p, 2i)$ such that $\tilde{\lambda}_p(\varphi_f \omega^{2i}) = 1$ and $v_p(\varphi_f \omega^{2i}) > 0$ ($v_p(\alpha) = e > 1$ or $v_p(\alpha^*) = e^* > 1$) or $\tilde{\lambda}_p(\varphi_f \omega^{2i}) = 2, 3$ among the above 171 981 262 pairs. For $p = 7$, $k = \mathbf{Q}(\sqrt{m}, \zeta_p + \zeta_p^{-1})$ and $1 < m < 1000$, a list of non-trivial cases ($v_p > 0$) was given in [22]. Our extended computation coincides with it.

$$\tilde{\lambda}_p(\varphi_f \omega^{2i}) = 1$$

$v_p(\varphi_f \omega^{2i}) = 1$

f	p	$2i$	f	p	$2i$	f	p	$2i$
12	701	542	21	199	150	33	53	30
37	43	32	53	1033	564	69	19	14
85	3697	3086	88	71	26	101	5333	2770
113	43	32	113	3373	1602	124	197	126
124	239	48	129	67	28	140	4751	120
141	5431	4826	149	43	32	149	71	16
149	229	182	157	401	56	161	101	22
168	37	22	172	73	10	173	43	32
173	101	42	181	71	52	181	6991	1628
185	827	354	188	1621	168	197	521	372

$v_p(\varphi_f \omega^{2i}) = 2$

f	p	$2i$
177	17	6

$v_p(\alpha) = e > 1$

f	p	$2i$	f	p	$2i$	f	p	$2i$
8	59	36	17	61	32	21	149	128
28	977	828	33	59	42	37	1091	812
41	7	4	41	283	102	44	787	148
53	7	2	53	1879	1158	57	2161	758
61	17	4	61	1747	1270	76	191	84
89	41	10	92	181	124	97	17	4
105	769	524	105	1453	162	120	2749	2196
124	41	30	140	107	74	149	797	140
149	2767	2178	152	17	12	168	43	10
173	13	4	177	31	24	184	373	72
193	7873	1886						

$v_p(\alpha^*) = e^* > 1$

f	p	$2i$	f	p	$2i$	f	p	$2i$
8	2221	1600	13	109	6	17	1319	88
28	223	126	33	31	24	33	1777	1184
41	19	12	41	421	126	60	19	14
61	7481	3516	73	11	2	73	1487	808
76	1451	418	76	4283	3484	97	367	26
109	41	32	133	1061	446	136	449	284
152	41	2	152	4027	3108	156	4637	2280
157	8221	582	165	29	26	165	89	66
165	1229	48	172	11	4	172	1487	900
177	337	74	184	1171	464	185	167	68
188	89	76						

$$\tilde{\lambda}_p(\varphi_f \omega^{2i}) = 2$$

f	p	$2i$	f	p	$2i$	f	p	$2i$
8	1151	842	21	11	4	24	29	4
24	181	84	29	569	64	37	5	2

37	89	66	37	3251	1094	40	257	232
44	653	448	53	193	14	56	1663	616
60	1277	582	60	1481	986	92	5	2
97	271	94	104	19	14	104	7919	4386
105	373	340	109	131	100	109	293	132
109	373	128	124	733	58	124	2111	1480
129	23	4	133	911	196	136	71	20
137	17	8	140	23	10	140	367	292
141	113	108	141	5939	2938	145	43	28
145	61	58	145	167	128	145	4157	3528
149	5	2	149	509	426	161	2389	646
165	11	2	172	13	10	172	47	38
173	7	4	177	157	48	181	223	26
185	17	6						

$$\tilde{\lambda}_p(\varphi_f\omega^{2i}) = 3$$

f	p	$2i$	f	p	$2i$
165	23	6	185	17	10

As in the argument of [26, pp. 158–159], we deduce that the number of exceptions to Vandiver's conjecture for $x_0 \leqslant p \leqslant x_1$ should be approximately $\frac{1}{2}(\log\log x_1 - \log\log x_0)$.

Let us use a similar naive approach. For $G_{\varphi_f\omega^{2i}}(T) = \sum_{j=0}^{\infty} a_j T^j$ and an integer c, we assume that the probability of $a_j \equiv c \bmod p^k$ is $1/p^k$. Further, for a cyclotomic unit c_0 with $d_0(c_0) \in \mathscr{U}_0^{p^e}$, we assume that the probability of $c_0 \in E_0^{p^k}$ is $1/p^k$ if $k \leqslant e$. Then, for a fixed conductor f and $x_0 \leqslant p \leqslant x_1$, we deduce that the number of pairs $(\varphi_f\omega^{2i}, p)$ such that $\tilde{\lambda}_p = 1$ and $v_p > 0$ ($e > 1$ or $e^* > 1$) should be approximately

$$\sum_{x_0 \leqslant p \leqslant x_1} \frac{p-3}{2}\left(\frac{1}{p} - \frac{1}{p^2}\right)\frac{1}{p}.$$

Let us apply this to our examples with $x_0 = 37$ and $x_1 = 10\,000$. Since the number of f's is 60, there should be about $60 \times 0.44645\cdots$ 'exceptions'. Our data does not seem to be much different from this number.

For $f = 1$ (i.e. the trivial character φ^0), the absolute value of the numerator N_{2i} of the Bernoulli number B_{2i} is generally smaller than that of the generalized Bernoulli number for $\varphi_f \neq \varphi^0$ and $2i$. We had better take this fact into consideration. For example, let $i = 1, 2, 3, 4, 5$ or 7. We easily see that $p \nmid N_{2i}$ for all $pn|i$. By Stickelberger's theorem, this implies that $A_0(\omega^{p-2i}) = \{0\}$ for all p. Further, by

Spiegelung relation, this implies that $A_0(\omega^{2i}) = \{0\}$. Moreover we have $A_0(\omega^{p-3}) = \{0\}$ for all p from the information on $K_4(\mathbf{Z})$ (see [21,25]). Therefore, excluding these i's, we deduce that 'the number of exceptions' to Vandiver's conjecture for $37 \leqslant p \leqslant q$ (q') might be smaller than E in the following table.

E	q	q'
0.1	113	149
0.2	419	450
0.3	1667	1737
0.4	8963	9058
0.5	67 807	68 096
0.6	799 417	800 172
0.7	16 224 227	16 224 227
0.8	640 612 703	640 492 743
0.9		$10^{10.75\cdots}$
1.0		$10^{13.13\cdots}$
1.5		$10^{35.71\cdots}$
2.0		$10^{97.07\cdots}$

Put $E_1(x) = \sum_{37 \leqslant p \leqslant x} \frac{p-17}{2} \left(\frac{1}{p}\right)^2$ and $E_2(x) = \frac{1}{2} \log \log x - 0.70476207 \cdots$, where the constant is selected to make $E_2(16\,224\,227)$ close to 0.7. We compute the first prime number q (resp. an approximation q') such that $E_1(q) > E$ (resp. $E_2(q') = E$).

Acknowledgments

The author wishes to express his gratitude to Professor H. Ichimura for valuable advice. He also wishes to express his gratitude to Professor T. Fukuda for valuable discussion on computation.

References

[1] J. Ax, On the units of an algebraic number field, Illinois J. Math. 9 (1965) 584–589.
[2] A. Brumer, On the units of algebraic number fields, Mathematika 14 (1967) 121–124.
[3] J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä, A.M. Shokrollahi, Irregular primes and cyclotomic invariants to 12 million, J. Symbolic Comput. 31 (2001) 89–96.
[4] B. Ferrero, L. Washington, The Iwasawa invariant μ_p vanishes for abelian number fields, Ann. Math. 109 (1979) 377–395.
[5] T. Fukuda, K. Komatsu, On $\mathbf{Z}_p$-extensions of real quadratic fields, J. Math. Soc. Japan 38 (1986) 95–102.
[6] T. Fukuda, K. Komatsu, A capitulation problem and Greenberg's conjecture on real quadratic fields, Math. Comput. 65 (1996) 313–318.
[7] T. Fukuda, H. Taya, The Iwasawa λ-invariants of $\mathbf{Z}_p$-extensions of real quadratic fields, Acta Arith. 69 (1995) 277–292.

[8] R. Gillard, Remarques sur les unités cyclotomiques et les unités elliptiques, J. Number Theory 11 (1979) 21–48.
[9] R. Greenberg, On the Iwasawa invariants of totally real number fields, Amer. J. Math. 98 (1976) 263–284.
[10] C. Greither, Class groups of abelian fields, and the main conjecture, Ann. Inst. Fourier (Grenoble) 42 (1992) 449–499.
[11] H. Ichimura, Local units modulo Gauss sums, J. Number Theory 68 (1998) 36–56.
[12] H. Ichimura, H. Sumida, On the Iwasawa invariants of certain real abelian fields II, Internat. J. Math. 7 (1996) 721–744.
[13] H. Ichimura, H. Sumida, On the Iwasawa invariants of certain real abelian fields, Tôhoku Math. J. 49 (1997) 203–215.
[14] H. Ichimura, H. Sumida, A note on integral bases of unramified cyclic extensions of prime degree II, Manuscripta Math. 98 (1999) 477–490.
[15] K. Iwasawa, A note on class numbers of algebraic number fields, Abh. Math. Sem. Univ. Hamburg 20 (1956) 257–258.
[16] K. Iwasawa, Lectures on p-adic L-functions, in: Annals of Mathematical Studies, Vol. 74, Princeton University Press, Princeton, NJ, 1972.
[17] K. Iwasawa, On $\mathbf{Z}_l$-extensions of algebraic number fields, Ann. Math. 98 (1973) 246–326.
[18] E. Knuth, The Art of Computer Programming, Vol. 2: Seminumerical Algorithms, 2nd Edition, Addison–Wesley, Reading, MA, 1981.
[19] J.S. Kraft, R. Schoof, Computing Iwasawa modules of real quadratic number fields, Compositio Math. 97 (1995) 135–155.
[20] T. Kubota, H.W. Leopoldt, Eine p-adische Theorie der Zetawerte, I. Einführung der p-adischen Dirichletschen L-Funktionen, J. Reine Angew. Math. 214/215 (1964) 328–339.
[21] M. Kurihara, Some remarks on conjectures about cyclotomic fields and K-groups of $\mathbf{Z}$, Compositio Math. 81 (1992) 223–236.
[22] M. Kurihara, The Iwasawa λ invariants of real abelian fields and the cyclotomic elements, Tokyo J. Math. 22 (1999) 259–277.
[23] B. Mazur, A. Wiles, Class fields of abelian extensions of $\mathbf{Q}$, Invent. Math. 76 (1984) 179–330.
[24] W. Sinnott, On the Stickelberger ideal and the circular units of an abelian field, Invent. Math. 62 (1980) 181–234.
[25] C. Soulé, Perfect forms and the Vandiver conjecture, J. Reine Angew. Math. 517 (1999) 209–221.
[26] L. Washington, Introduction to Cyclotomic Fields, 2nd Edition, Graduate Texts in Mathematics, Vol. 83, Springer, New York, 1997.
[27] A. Wiles, The Iwasawa conjecture for totally real fields, Ann. Math. 131 (1990) 493–540.